(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号

特開平10－117173

(43)公開日　平成10年(1998)５月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｈ	1/00	Ｈ０４Ｈ	1/00　Ｆ
Ｈ０４Ｋ	1/00	Ｈ０４Ｋ	1/00　Ｚ
Ｈ０４Ｎ	7/16	Ｈ０４Ｎ	7/16　Ｃ
	7/167		7/167　Ｚ

審査請求　未請求　請求項の数11　ＯＬ　（全 10 頁）

(21)出願番号　特願平8－269938

(22)出願日　平成８年(1996)10月11日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　早川　和宏
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　福永　博信
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　渡部　智樹
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　若林　忠

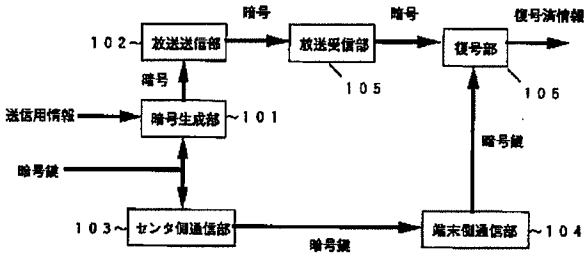
最終頁に続く

(54)【発明の名称】　情報配信装置および情報受信装置

(57)【要約】

【課題】　暗号化された情報を多数の利用者に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険を小さくする。

【解決手段】　暗号生成部１０１は送信用情報と暗号鍵を受け取り、送信用情報を暗号化して出力する。放送送信部１０２は暗号を受け取り不特定多数に対して放送する。センタ側通信部１０３は暗号鍵を受け取り、通信路を通じて送信する。端末側通信部１０４は通信路を通じて暗号鍵を受け取り、出力する。放送受信部１０５は放送された暗号を受信し出力する。復号部１０６は暗号と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が入力されない場合は動作を行わない。



【特許請求の範囲】

【請求項１】　情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する情報配信装置。

【請求項２】　情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する情報配信装置。

【請求項３】　請求項１の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項４】　前記暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する請求項３記載の情報受信装置。

【請求項５】　請求項２の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項６】　前記照合情報は前記暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて前記情報配信装置との通信路の接続／切断を行なう通信路制御手段を有する、請求項５記載の情報受信装置。

【請求項７】　請求項２の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報に関する関連情報と前記照合情報を得て両者を照合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項８】　請求項２の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む前記照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報を含む情報から暗号化された前記情報に関する関連情報を分離する関連情報分離手段と、前記関連情報と前記照合情報を得て両者を照合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項９】　前記関連情報は、暗号化された情報の情報識別子を含み、前記照合情報は、復号できる情報の情報識別子を一つ以上含み、前記照合情報出力手段は前記照合情報に含まれる情報識別子の中に、前記関連情報に含まれる情報識別子が含まれていることを、前記照合情報を出力する条件とする請求項８記載の情報受信装置。

【請求項１０】　前記関連情報は、暗号化された情報の秘匿度を表す数値を含み、前記照合情報は、復号できる情報の秘匿度を表す数値を含み、前記照合情報出力手段は前記関連情報に含まれる秘匿度が、前記照合情報に含まれる秘匿度以下であることを、前記照合情報を出力する条件とする請求項８記載の情報受信装置。

【請求項１１】　前記関連情報は、暗号の復号方法を指示する情報を含み、前記照合情報出力手段は前記関連情報に含まれる暗号の復号方法に従い前記照合情報受信手段を制御して照合情報を取得する請求項８記載の情報受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報を暗号化して不特定多数に対して放送し、受信者のみが受信した暗号化された情報を復号する情報配信・受信システムに関する。

【０００２】

【従来の技術】放送において受信者を限定したい場合、放送内容を暗号化して暗号鍵を持つものだけが暗号を復号して放送内容を知ることができるようにするのが一般的である。たとえば、有料放送では放送内容を暗号化し、受信料を支払う受信者のみが暗号を復号することができるようにする必要がある。これを実現するため、従来は復号装置に付加するハードウェアを用意しこれに暗号鍵を記録したものか、あるいは復号装置の一部もしくは全体を、暗号を復号する権利のある者に提供する方法が採られていた。

【０００３】また、有料放送のように「見た分だけ課金する」ことが必要な場合は、復号操作を行ったことに対する課金処理、または復号を行った際の料金徴収者への通知を自動的に行えることが望ましい。このため、暗号を復号する装置においては、暗号が復号される条件を情報提供者の側で制御することができるか、あるいは暗号が復号されたことを確実に情報提供者に伝えることができる装置が要求される。従来、この目的のためには復号操作を行ったことをＩＣカードなどのハードウェアに記録し、この記録を情報提供者が定期的に回収することで課金等を行っていた。

【０００４】
【発明が解決しようとする課題】これらの方法は、復号装置や暗号鍵の複製により、復号する権利のない者が復号を行う可能性や、ＩＣカードに記録されたデータを改変され、正常に課金が行えない可能性があった。また、ＩＣカードその他の付加的なハードウェアに対するコスト、復号操作を行った記録を回収するコスト等がかかり、有料情報提供サービスのコストアップの原因となっていた。
【０００５】本発明の目的は、暗号化された情報を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい情報配信装置および情報受信装置を提供することにある。
【０００６】
【課題を解決するための手段】本発明の第１の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する。また、本発明の第１の情報受信装置は、放送された情報を含む情報を受信する放送受信手段と、暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。
【０００７】このシステムでは利用者は暗号と暗号鍵を常に受信しているので、送信側では任意の時刻に暗号鍵を変更することができる。したがって、多数の利用者へ暗号を放送することにより情報配信を行う際に、暗号鍵の複製や不正使用が行われる危険を小さくすることができる。
【０００８】本発明の実施態様によれば、暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する。
【０００９】回線断後も暗号鍵を保持することができるので、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、この装置が有用である。
【００１０】本発明の第２の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する。本発明の第２の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。
【００１１】本発明の実施態様によれば、情報受信装置は、照合情報が暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて情報配信装置との通信路の接続／切断を行なう通信路制御手段を有する。これによりシステムの運用上の利便性が高まる。
【００１２】本発明の第３の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報に関する関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。
【００１３】あらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。
【００１４】本発明の第４の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報を含む情報から暗号化されている情報に関する関連情報を分離する関連情報分離手段と、関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。
【００１５】本発明の実施態様によれば、関連情報は、暗号化されている情報の情報識別子を含み、照合情報は、復号できる情報の情報識別子を一つ以上含み、照合情報出力手段は照合情報に含まれる情報識別子の中に、関連情報に含まれる情報識別子が含まれていることを、照合情報を出力する条件とする。
【００１６】本発明の実施態様によれば、関連情報は、暗号化されている情報の秘匿度を表す数値を含み、照合情報は、復号できる情報の秘匿度を表す数値を含み、照合情報出力手段は関連情報に含まれる秘匿度が、照合情報に含まれる秘匿度以下であることを、照合情報を出力する条件とする。
【００１７】暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。
【００１８】本発明の実施態様によれば、関連情報は、暗号の復号方法を指示する情報を含み、照合情報出力手段は関連情報に含まれる暗号の復号方法に従い照合情報受信手段を制御して照合情報を取得する。
【００１９】照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。
【００２０】
【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。
【００２１】図１は本発明の第１の実施形態の情報配信・受信システムの構成を示すブロック図である。

【００２２】暗号生成手段である暗号生成部１０１は送信用情報と暗号鍵を受け取り、送信用情報を暗号化して出力する。放送送信手段である放送送信部１０２は暗号化された情報を受け取り、不特定多数に対して放送する。暗号鍵送信手段を含むセンタ側通信部１０３は暗号鍵を受け取り、通信路を通じて送信する。暗号鍵受信手段を含む端末側通信部１０４は通信路を通じて暗号鍵を受け取り、出力する。放送受信手段である放送受信部１０５は放送された暗号化された情報を受信し、出力する。復号手段である復号部１０６は暗号化された情報と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が入力されない場合は動作を行わない。ここで、暗号生成部１０１と放送送信部１０２とセンタ側通信部１０３は情報配信装置を構成し、放送受信部１０５と端末側通信部１０４と復号部１０３は情報受信装置を構成している。

【００２３】したがって、図１のシステムでは通信を行って暗号鍵を受信してる間だけ復号部１０６が動作する。

【００２４】このシステムでは、その時点で送信される暗号と対応しているかぎりにおいて、暗号鍵を任意の時間に変化させてよい。したがって、受信側では情報を復号する必要がある間、常に通信路を通じて暗号鍵を受け取り続ける必要がある。

【００２５】なお、通信路としては、端末側からセンタ側へ情報を送る必要はないので、一般的な双方向通信サービスのほか、同報通信サービスを利用することができる。

【００２６】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる通信サービスを利用する場合には、受信者が暗号鍵を受信したことを確認できる。したがって、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。

【００２７】図２は本発明の第２の実施形態の情報配信・受信システムの構成を示すブロック図である。

【００２８】暗号生成手段である情報サーバ２０１は送信したい情報を受け取って暗号化し、放送送信手段である送信装置２０２を通じて放送用衛星に向けて送信する。また同時に、暗号鍵を暗号鍵送信手段であるモデム２０３を通じて専用線による通信路へ送出する。放送受信手段である受信装置２０５は衛星からの電波を受信し、暗号化された情報を出力する。同時に、暗号鍵受信手段であるモデム２０４は通信路から暗号鍵を受信し、出力する。復号手段である復号部２０６は暗号化された情報を暗号鍵を用いて解読し、復号済み情報を出力する。ここで、情報サーバ２０１と送信装置２０２とモデム２０３は情報配信装置を構成し、モデム２０４と受信装置２０５と復号部２０６は情報受信装置を構成している。

【００２９】情報サーバ２０１は任意の時間に暗号鍵を変更する。したがって、暗号を持続的に復号することができるのは通信路に接続されている情報受信装置のみとなる。

【００３０】以上の説明では通信路として専用線を想定したが、通常の電話回線やＣＡＴＶ回線も使用可能である。

【００３１】なお、端末側通信部１０５、モデム２０４は、回線断後も暗号鍵を保持するようにしてもよい。この場合、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、有用である。

【００３２】図３は本発明の第３の実施形態の情報配信・受信システムの構成を示すブロック図である。

【００３３】暗号生成部３０１、放送送信部３０２、放送受信部３０５、復号部３０８の機能はそれぞれ図１中の暗号生成部１０１、放送送信部１０２、放送受信部１０５、復号部１０６の機能と同様である。

【００３４】照合情報生成部３０３は暗号鍵を受け取り、暗号鍵に任意の情報を付加した照合情報を生成し、出力する。照合情報送信手段であるセンタ側通信部３０４は照合情報を受け取り、通信路を通じて送信する。照合情報受信手段である端末側通信部３０６は通信路を通じて照合情報を受け取り、出力する。暗号鍵分離手段である暗号鍵抽出部３０７は照合情報を受け取り、暗号鍵を抽出して出力する。ここで暗号生成部３０１、放送送信部３０２、照合情報生成部３０３、センタ側通信部３０４は情報配信装置を構成し、放送受信部３０５、端末側通信部３０６、暗号鍵抽出部３０７、復号部３０８は情報受信装置を構成している。

【００３５】本システムでは、暗号鍵に関する付加情報を照合情報に含めて通信する。付加情報としては暗号鍵が作成された時刻、暗号鍵の有効期間、復号アルゴリズム識別子、放送サービスのサービス識別子、サービス提供者識別子などを用いることができる。端末側通信部３０６が照合情報を保持できる場合は、照合情報の中に例えば暗号鍵の有効期間を含めておき、受信側の通信路制御手段でこれを参照して暗号鍵の有効期間が切れるまでは通信回線を切断しておくことができる。

【００３６】図４は本発明の第４の実施形態の情報配信・受信システムの構成を示すブロック図である。

【００３７】暗号生成部４０１、放送送信部４０２、照合情報生成部４０３、センタ側通信部４０４、端末側通信部４０６、暗号鍵抽出部４０８、放送受信部４０５、復号部４０９の機能はそれぞれ図３中の暗号生成部３０１、放送送信部３０２、照合情報生成部３０３、センタ側通信部３０４、端末側通信部３０６、暗号鍵抽出部３０７、放送受信部３０５、復号部３０８の機能と同様である。

【００３８】照合情報出力手段である照合部４０７は関連情報と照合情報を受け取り、照合情報と関連情報を比較して復号が許可される場合のみ照合情報を出力する。

【００３９】ここで、暗号生成部４０１、放送送信部４０２、照号情報生成部４０３、センタ側通信部４０４は情報配信装置を構成し、放送受信部４０５、端末側通信部４０６、照合部４０７、暗号鍵抽出部４０８、復号部４０９は情報受信装置を構成している。

【００４０】照合情報と関連情報は暗号化されている情報の復号を許可するか否かにかかわる情報を用いることができる。たとえば照合情報で送られたパスワードと関連情報で入力されたパスワードが一致した場合のみ復号を許可するという使い方が可能である。この場合は、一般に行われているように、照合情報で送信するパスワードは逆変換が不可能な演算をあらかじめ施してから送信し、関連情報に対して同じ演算を行った結果と比較すれば、照合情報の中からパスワードを盗まれる危険はない。

【００４１】図１から図３のシステムでは通信回線に接続できれば必ず暗号を復号することができるが、図４のシステムではあらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。

【００４２】図５は本発明の第５の実施形態の情報配信・受信システムの構成を示すブロック図である。

【００４３】暗号生成部５０１、照合情報生成部５０３、センタ側通信部５０４、端末側通信部５０５、暗号鍵抽出部５０９、復号部５１０の機能は図４中のそれぞれ暗号生成部４０１、照合情報生成部４０３、センタ側通信部４０４、端末側通信部４０６、暗号鍵抽出部４０８、復号部４０９の機能と同様である。

【００４４】放送送信手段である放送送信部５０２は暗号化された情報と関連情報を受け取り、両者を含む放送信号を生成し、不特定多数に対して放送する。放送受信手段である放送受信部５０６は放送信号を受信し出力する。関連情報分離手段である関連情報分離部５０７は放送信号を受け取り、暗号と関連情報を抽出して出力する。照合情報出力手段である照合部５０８は関連情報と照合情報を比較し、比較結果により復号が許可される場合のみ照合情報を出力する。

【００４５】ここで、暗号生成部５０１、放送送信部５０２、照合情報生成部５０３、センタ側通信部５０４は情報配信装置を構成し、端末側通信部５０５、放送通信部５０６、関連情報分離部５０７、照合部５０８、暗号抽出部５０９、復号部５１０は情報受信装置を構成している。

【００４６】関連情報は暗号化されている情報に関する情報である。たとえば暗号に含まれている情報を表す情報識別子、情報の秘匿度を表す数値などである。一方、照合情報は暗号鍵の他に、関連情報と対応する復号許可情報を含む。復号許可情報は暗号鍵が用いられる条件を記述した情報である。例としては、一つまたは複数の情報を表す情報識別子や復号できる情報の秘匿度を表す数値などである。

【００４７】照合情報生成部５０３を複数用いてそれぞれが異なる情報識別子や情報秘匿度を含む照合情報を生成し、異なる通信チャネルを用いて送信すれば、受信側が復号できる情報を、どの通信チャネルに接続するかにより決定することができる。

【００４８】図６は本発明の第６の実施形態の情報配信・受信システムの構成を示すブロック図である。このシステムはＣＳ放送においてスクランブル暗号化されたＭＰＥＧ２パケットの暗号鍵を通信路を通じて取得する。ここでは通信路として電話回線を想定する。また、このシステムでは放送番組と共にその番組の種類に関する情報が放送される。一方、通信路では暗号鍵のほかにその暗号鍵を使用できる番組の種類を送信する。受信側では、この番組の種類に従って、暗号を復号するか否かを決定する。

【００４９】タイマ６０１は一定時間毎に暗号鍵更新要求を出力する。暗号鍵生成部６０２は暗号鍵更新要求を受けると新しい暗号鍵を生成し出力する。照合情報生成部６０５は暗号鍵に許可する番組の種類を付加して出力する。図７は照合情報に用いる番組の種類に関する情報の一例を示す図である。生成された照合情報はモデム６０６を通じて通信路へ送信される。照合情報は、一つのセンタから複数の利用者へ送信する必要があるため、同報型の通信サービスを利用する。暗号生成手段である暗号生成部６０３は暗号鍵とＭＰＥＧ符号を受け取り暗号を生成して出力する。放送送信手段であるＣＳ放送装置６０４は関連情報と暗号を受け取り、放送パケットとして衛星を通じて放送する。関連情報には図７と同じ形式で現在放送中の番組のジャンルを示す情報が含まれる。放送受信手段であるＣＳ受信装置６０８は衛星からの放送を受信し放送パケットを出力する。関連情報分離手段である関連情報分離部６１１は放送パケットを受け取り、関連情報と暗号を分離し、出力する。受信側モデム６０７は照合情報を通信路から受信し出力する。照合情報出力手段である照合部６０９は照合情報と関連情報を受け取り、関連情報中の番組ジャンルが照合情報中の番組ジャンルに含まれていれば照合情報を出力する。暗号鍵分離手段である暗号鍵抽出部６１０は照合情報から暗号鍵を抽出し出力する。復号手段である復号部６１２は暗号と暗号鍵を受け取り、暗号を復号して得られるＭＰＥＧ符号を出力する。

【００５０】ここで、タイマ６０１、鍵生成部６０２、暗号生成部６０３、ＣＳ放送装置６０４、照合情報生成部６０５、モデム６０６は情報配信装置を構成し、モデム６０７、ＣＳ受信装置６０８、照合部６０９、暗号鍵抽出部６１０、関連情報分離部６１１、復号部６１２は

情報受信装置を構成している。

【００５１】以上の説明では関連情報と照合情報には番組のジャンルに関する情報を持たせたが、ジャンル以外の情報を持たせることもできる。図８は関連情報に番組識別子、照合情報に複数の番組識別子のリストを持たせ、リストに示された番組のみ復号可とする例である。また、図９は関連情報には番組のレベル、照合情報にはその照合情報で復号を許可する番組のレベルを持たせ、そのレベル以下の番組のみ復号可とする例である。

【００５２】また、図６において関連情報の中に照合情報を入手する際に必要な同報型通信サービスの電話番号を含めておけば、モデム６０７をこの電話番号に対して発呼するよう制御することにより、照合情報の入手先が目的に応じて複数存在しても、自動的に照合情報を取得することができる。

【００５３】

【発明の効果】以上説明したように、本発明は、下記のような効果がある。

（１）請求項１と３の発明は、暗号の復号に必要な暗号鍵を頻繁に変更することができるので、暗号化された情報を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい。

【００５４】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる場合には、受信者が暗号鍵を受信したことを確認できるので、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。これは有料放送をスクランブラ／デスクランブラを用いて行う際に、見た分だけ課金することを可能にする。

（２）請求項４の発明は、請求項１と３からなるシステムの機能を短い通信時間で実現することができる。

（３）請求項２と５と６の発明は、暗号鍵の有効期間など付加的な情報を通信することにより、装置の運用上の利便性を高めることができる。

（４）請求項２と７の発明は、復号を行う際に、復号を行う者が正しい利用者かどうかを受信者の側で試験することができる。

（５）請求項８、９、１０の発明は、暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。この機能は、ある特定の情報を、特定の受信者集合に対して、復号を許可するかどうかを送信側で指定するために用いることができる。たとえば有料放送で、ある一定の課金額の通信チャネルを通じて暗号鍵を取得している利用者が、どの番組を視聴することができるかを指定することができる。

（６）請求項１１の発明は、照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図２】本発明の第２の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図３】本発明の第３の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図４】本発明の第４の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図５】本発明の第５の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図６】本発明の第６の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図７】本発明の第５、第６の実施形態において照合情報に含まれる情報の例を示す図である。

【図８】本発明の第５、第６の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

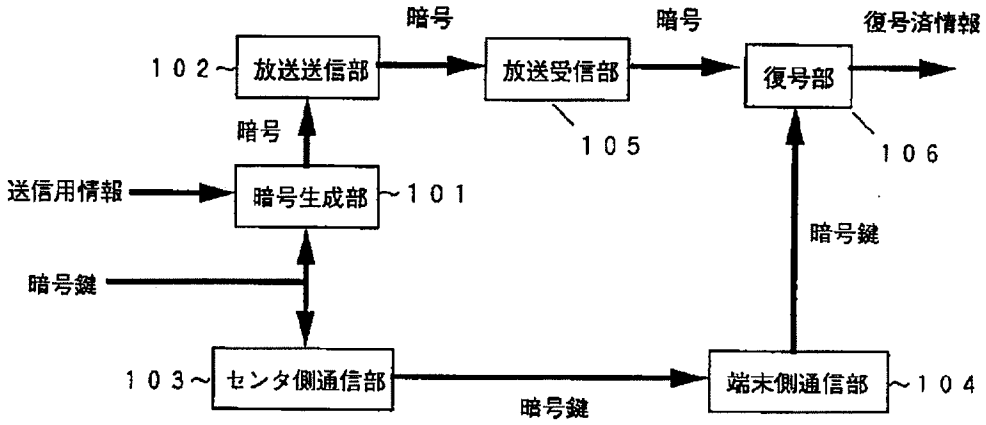
【図９】本発明の第５、第６の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

【符号の説明】

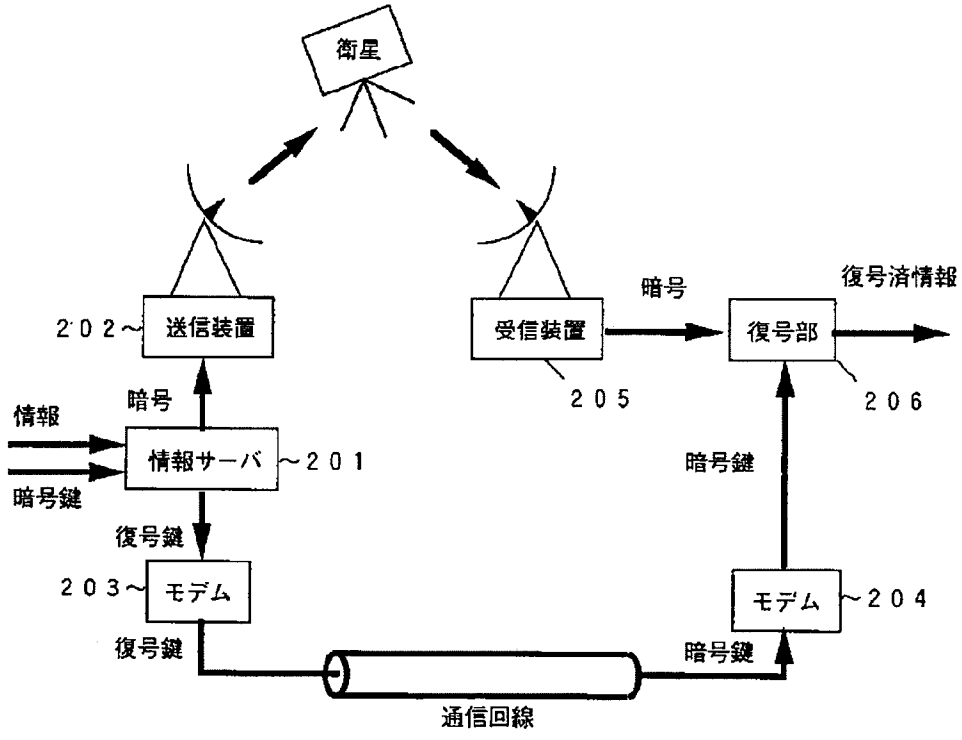
１０１　暗号生成部
１０２　放送送信部
１０３　センタ側通信部
１０４　端末側通信部
１０５　放送受信部
１０６　復号部
２０１　情報サーバ
２０２　送信装置
２０３　モデム
２０４　モデム
２０５　受信装置
２０６　復号装置
３０１　暗号生成部
３０２　放送送信部
３０３　照合情報生成部
３０４　センタ側通信部
３０５　放送受信部
３０６　端末側通信部
３０７　暗号鍵抽出部
３０８　復号部
４０１　暗号生成部
４０２　放送送信部
４０３　照合情報生成部
４０４　センタ側通信部
４０５　放送受信部
４０６　端末側通信部
４０７　照合部
４０８　暗号鍵抽出部
４０９　復号部

５０１　暗号生成部
５０２　放送送信部
５０３　照合情報生成部
５０４　センタ側通信部
５０５　端末側通信部
５０６　放送受信部
５０７　関連情報分離部
５０８　照合部
５０９　暗号鍵抽出部
５１０　復号部
６０１　タイマ
６０２　暗号鍵生成部
６０３　暗号生成部
６０４　ＣＳ放送装置
６０５　照合情報生成部
６０６　モデム
６０７　モデム
６０８　ＣＳ受信装置
６０９　照合部
６１０　暗号鍵抽出部
６１１　関連情報分離部
６１２　復号部

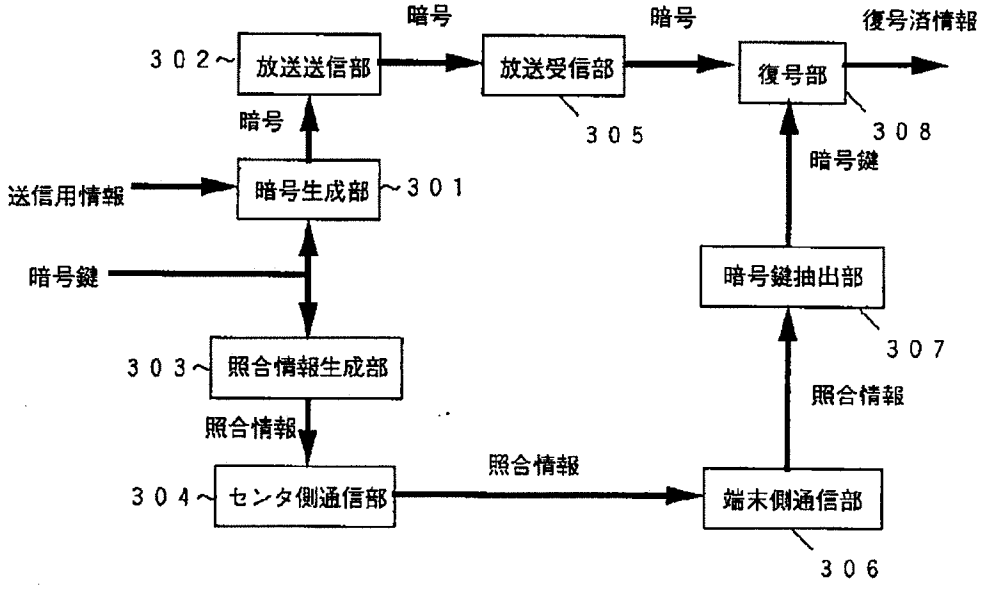
【図１】



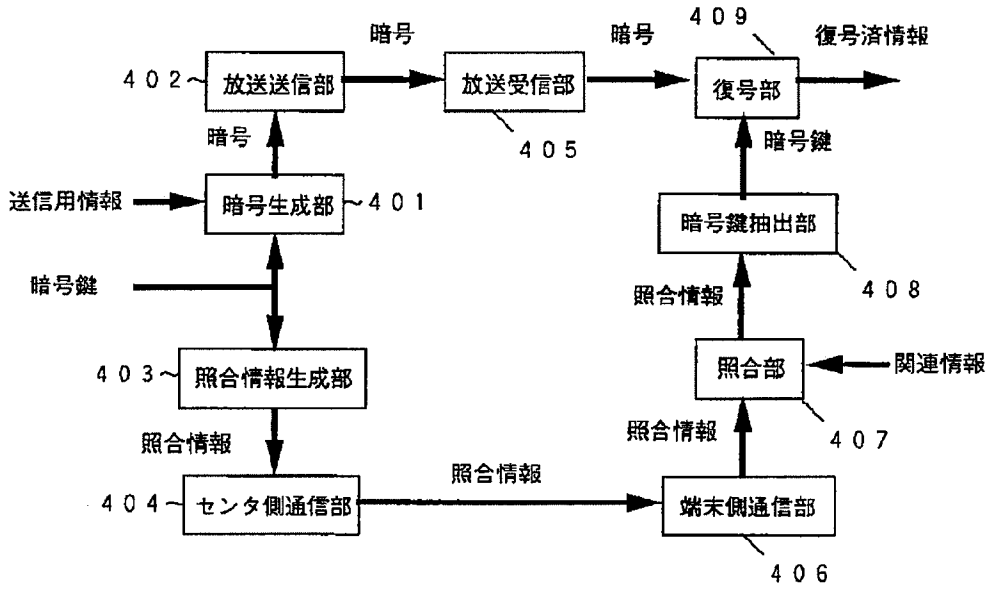
【図２】



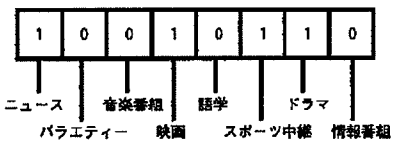
【図3】


暗号
暗号
復号済情報
302～
放送送信部
放送受信部
復号部
305
308
暗号
暗号鍵
送信用情報
暗号生成部
～301
暗号鍵
暗号鍵抽出部
307
303～
照合情報生成部
照合情報
照合情報
照合情報
304～
センタ側通信部
端末側通信部
306

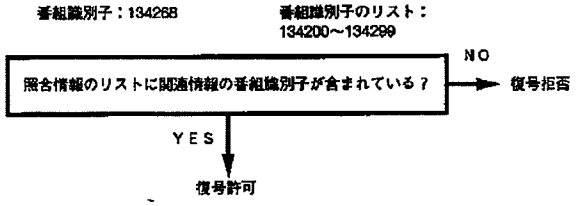
【図4】


暗号
暗号
409
復号済情報
402～
放送送信部
放送受信部
復号部
405
暗号
暗号鍵
送信用情報
暗号生成部
～401
暗号鍵抽出部
408
暗号鍵
照合情報
照合部
関連情報
403～
照合情報生成部
照合情報
照合情報
407
照合情報
404～
センタ側通信部
端末側通信部
406

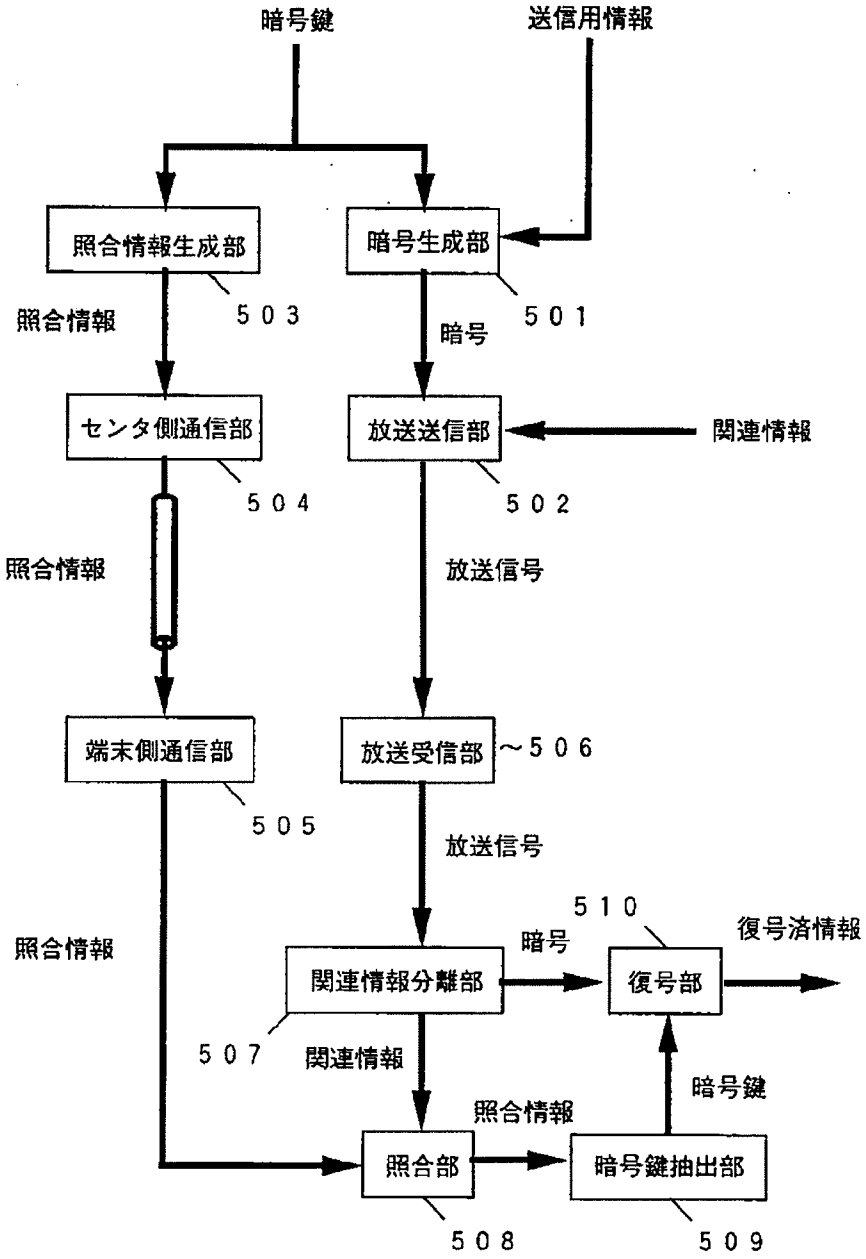
【図7】


1
0
0
1
0
1
1
0
ニュース
バラエティー
音楽番組
映画
語学
スポーツ
ドラマ
中継
情報番組

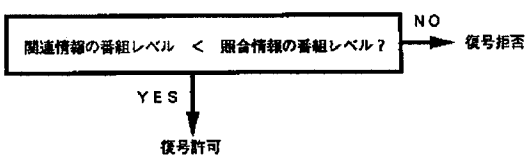
【図8】


関連情報
番組識別子：134268
照合情報
番組識別子のリスト：
134200～134299
照合情報のリストに関連情報の番組識別子が含まれている？
NO
復号拒否
YES
復号許可

【図5】



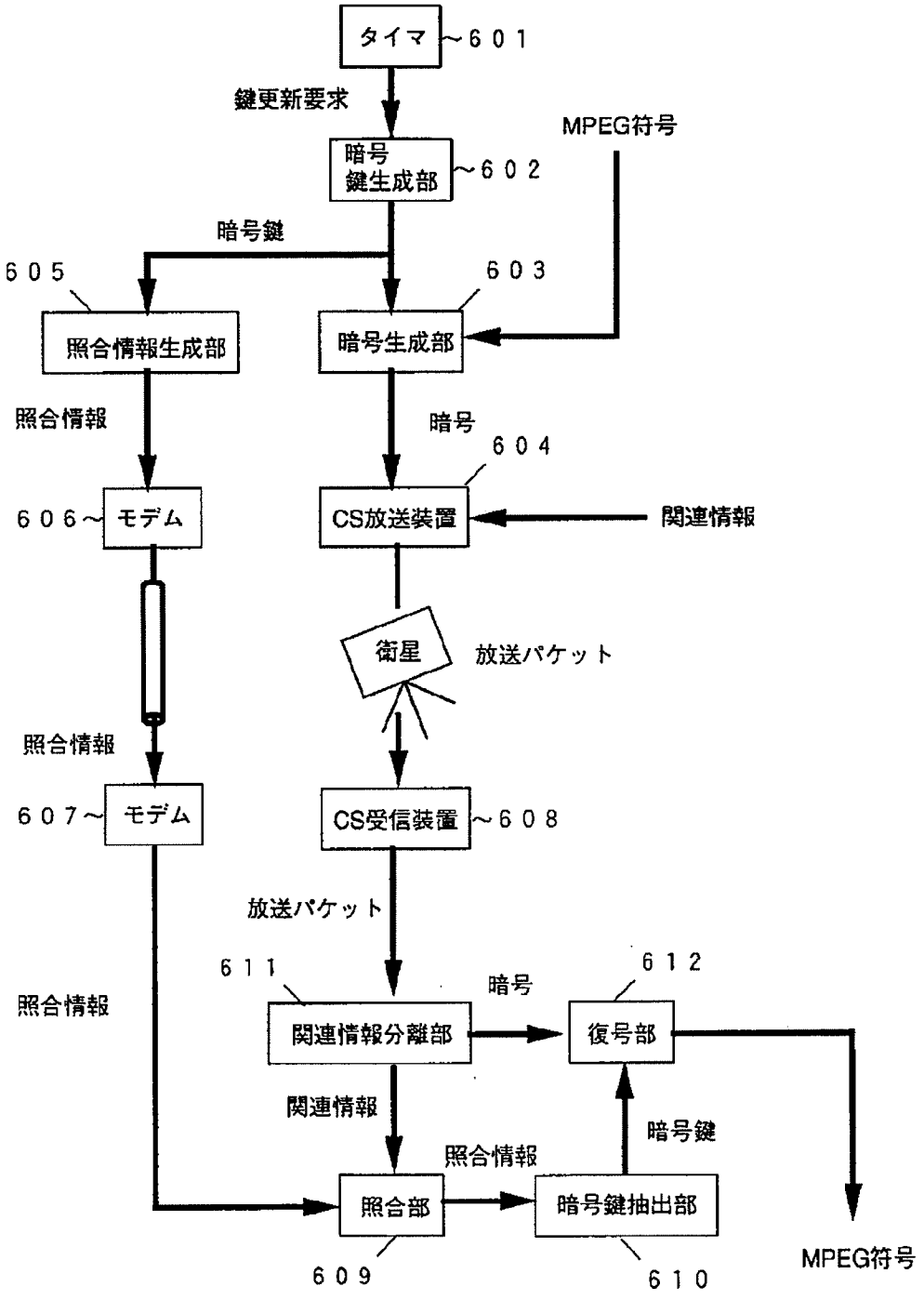
【図9】



番組レベルの例

レベル1：映画、スポーツ中継、バラエティを除く全番組
レベル2：映画、スポーツ中継を除く全番組
レベル3：スポーツ中継を除く全番組
レベル4：全番組

【図６】



フロントページの続き

(72)発明者　鈴木　達郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　熊谷　佳子
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-117173
(43)Date of publication of application : 06.05.1998

(51)Int.Cl. H04H 1/00
H04K 1/00
H04N 7/16
H04N 7/167

(21)Application number : 08-269938
(22)Date of filing : 11.10.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HAYAKAWA KAZUHIRO
FUKUNAGA HIRONOBU
WATABE TOMOKI
SUZUKI TATSURO
KUMAGAI YOSHIKO

(54) INFORMATION DISTRIBUTER AND INFORMATION RECEIVER

(57)Abstract:
PROBLEM TO BE SOLVED: To lessen the danger that an illegal user decodes encrypted information or copies an encryption key in the case that encrypted information is distributed to a large number of users.
SOLUTION: An encryption generating section 101 receives transmission information and an encryption key and encrypts the transmission information and provides an output of the result. A broadcast transmission section 102 receives the encrypted information and broadcasts the information to a large number of unspecified persons. A center side communication section 104 receives the encryption key and sends it to a communication channel. A terminal equipment side communication section 104 receives the encryption key through the communication channel and provides an output of it. A broadcast reception section 105 receives the broadcast encrypted information and provides an output of it. A decoding section 106 receives the encrypted information and the encryption key and provides an output of decoded information but is not operative when the section 106 receives no encryption key.

CLAIMS

[Claim(s)]
[Claim 1]An information distributing device which enciphers and distributes

informationcomprising:
A cipher generation means which obtains information and an encryption key and enciphers said information.
A broadcast transmitting means which broadcasts information including said enciphered information.
An encryption key transmitting means which transmits said encryption key through a channel.

[Claim 2]An information distributing device which enciphers and distributes informationcomprising:
A cipher generation means which obtains information and an encryption key and enciphers said information.
A broadcast transmitting means which broadcasts information including said enciphered information.
A collation information transmitting means which transmits collation information containing said encryption key through a channel.

[Claim 3]An information reception device which receives information enciphered with an information distributing device of claim 1comprising:
A broadcast receiving means which receives information including enciphered information.
An encryption key reception means which receives said encryption key through a channel.
A decoding means which decodes said information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 4]The information reception device according to claim 3 which holds an old encryption key until an encryption key with said new encryption key reception means is obtained.
[Claim 5]An information reception device which receives information enciphered with an information distributing device of claim 2comprising:
A broadcast receiving means which receives information including enciphered information.
A collation information reception means which receives collation information containing said encryption key through a channel.
Encryption key separating mechanism which separates said encryption key from said collation information.
A decoding means which decodes information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 6]The information reception device according to claim 5 with which said collation information has a channel control means which performs connection/cutting of a channel with said information distributing device based on information on this shelf-life including information on a shelf-life of said encryption

key.
[Claim 7]An information reception device which receives information enciphered with an information distributing device of claim 2comprising:
A broadcast receiving means which receives information including enciphered information.
A collation information reception means which receives collation information containing said encryption key through a channel.
A collation information output means which outputs said collation information only when pertinent information about said enciphered information and said collation information are acquiredboth are compared and decoding is permitted.
Encryption key separating mechanism which separates said encryption key from said collation informationand a decoding means which decodes information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 8]An information reception device which receives information enciphered with an information distributing device of claim 2comprising:
A broadcast receiving means which receives information including enciphered information.
A collation information reception means which receives said collation information containing said encryption key through a channel.
Pertinent information separating mechanism which separates pertinent information about said information enciphered from information including said enciphered information.
A collation information output means which outputs said collation information only when said pertinent information and said collation information are acquiredboth are compared and decoding is permittedencryption key separating mechanism which separates said encryption key from said collation informationand a decoding means which decodes said information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 9]Said pertinent information including an information identifier of enciphered information said collation informationThe information reception device according to claim 8 which makes it conditions which output said collation information to include one or more information identifiers of information which can be decodedand to contain an information identifier contained in said pertinent information in an information identifier by which said collation information output means is included in said collation information.
[Claim 10]Said pertinent information the degree of secrecy of enciphered information including a numerical value to express said collation informationThe information reception device according to claim 8 which includes a numerical value showing the degree of secrecy of information which can be decodedand makes it conditions which output said collation information for said collation information output means to be below the degree of secrecy by which the degree of secrecy contained in said pertinent information is contained in said collation information.

[Claim 11]The information reception device according to claim 8 which said pertinent information includes information which directs a decoding method of a codeand said collation information output means controls said collation information reception means in accordance with a decoding method of a code contained in said pertinent informationand acquires collation information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention enciphers informationbroadcasts it to many and unspecified personsand relates to the information distribution receiving system which decodes the enciphered information which only the addressee received.
[0002]
[Description of the Prior Art]It is common only for what enciphers contents of broadcast and has an encryption key to decode a codeand to enable it to get to know contents of broadcast to limit an addressee in broadcast. For examplecontents of broadcast are enciphered and only the addressee who pays a subscription fee needs to enable it to decode a code in paid broadcasting. In order to realize thisor it would not prepare conventionally the hardware added to a decoding device and would not record an encryption key on thisthe method of providing with some or the whole of a decoding device a person with the right to decode a code was taken.
[0003]When what "only a part to have seen is charged for" like paid broadcasting is requiredit is desirable that a notice to the rate collection person at the time of performing accounting to having performed decoding operation or decoding can be performed automatically. For this reasonin the device which decodes a codethe device which can tell an information provider certainly that could control the conditions by which a code is decoded by the information provider sideor the code was decoded is required. It recorded having performed decoding operation conventionally for this purpose on hardwaressuch as an IC cardand fee collection etc. were performed because an information provider collects these records periodically.
[0004]
[Problem(s) to be Solved by the Invention]These methods had a possibility that a person without the right to decode will decode by the duplicate of a decoding device or an encryption keyand the data recorded on the IC card changedand may be unable to be charged normally. The cost to the hardware in which others are [being an IC card and] additionalthe cost which collects the records which performed decoding operationetc. startedand it had become a cause of the cost hike of pay information providing service.
[0005]When the purpose of this invention distributes the enciphered information to

many users simultaneouslythere is a risk of an inaccurate user decoding or reproducing an encryption key in providing a small information distributing device and an information reception device.
[0006]
[Means for Solving the Problem]The 1st information distributing device of this invention is provided with the following.
A cipher generation means which obtains information and an encryption key and enciphers said information.
A broadcast transmitting means which broadcasts information including enciphered information.
An encryption key transmitting means which transmits an encryption key through a channel.
The 1st information reception device of this invention is provided with the following.
A broadcast receiving means which receives information including broadcast information.
An encryption key reception means which receives an encryption key through a channel.
A decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0007]In this systemsince a user has always received a code and an encryption keyhe can change an encryption key at arbitrary time in the transmitting side. Thereforewhen performing distribute information by broadcasting a code to many usersa risk of a duplicate and an unauthorized use of an encryption key being performed can be made small.
[0008]According to the embodiment of this inventionan encryption key reception means holds an old encryption key until a new encryption key is obtained.
[0009]Since after disconnection can hold an encryption keyit can continue decoding until an encryption key changes nexteven if it cuts a communication line. When using a telephone line as a communication linea point of telex rate gold reduction to this device is useful.
[0010]The 2nd information distributing device of this invention is provided with the following.
A cipher generation means which obtains information and an encryption key and enciphers said information.
A broadcast transmitting means which broadcasts information including enciphered information.
A collation information transmitting means which transmits collation information containing an encryption key through a channel.
The 2nd information reception device of this invention is provided with the following.
A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing an encryption key through a channel.
Encryption key separating mechanism which separates an encryption key from collation information.
A decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0011]As for an information reception deviceaccording to the embodiment of this inventioncollation information has a channel control means which performs connection/cutting of a channel with an information distributing device based on information on this shelf-life including information on a shelf-life of an encryption key. Therebyconvenience on employment of a system increases.
[0012]The 3rd information reception device of this invention is provided with the following.
A broadcast receiving means which receives information including enciphered information.
A collation information reception means which receives collation information containing an encryption key through a channel.
A collation information output means which outputs collation information only when pertinent information and collation information about enciphered information are acquiredboth are compared and decoding is permitted.
Encryption key separating mechanism which separates an encryption key from collation informationand a decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0013]Since it can restrict when an addressee has obtained right pertinent information beforehandand it can decodean addressee of information can be limited more.
[0014]The 4th information reception device of this invention is provided with the following.
A broadcast receiving means which receives information including enciphered information.
A collation information reception means which receives collation information containing an encryption key through a channel.
Pertinent information separating mechanism which separates pertinent information about information enciphered from information including enciphered information.
A collation information output means which outputs collation information only when pertinent information and collation information are acquiredboth are compared and decoding is permittedencryption key separating mechanism which separates an encryption key from collation informationand a decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0015]According to the embodiment of this inventionpertinent information including an information identifier of information enciphered collation informationOne or more information identifiers of information which can be decoded are includedand a collation information output means makes it conditions which output collation information to contain an information identifier contained in pertinent information in an information identifier contained in collation information.
[0016]According to the embodiment of this inventionpertinent information the degree of secrecy of information enciphered including a numerical value to express collation informationIncluding a numerical value showing the degree of secrecy of information which can be decodeda collation information output means makes it conditions which output collation information for the degree of secrecy contained in pertinent information to be below the degree of secrecy contained in collation information.
[0017]It can examine without whether a code is a thing corresponding to an encryption keyand decoding.
[0018]According to the embodiment of this inventionpertinent information includes information which directs a decoding method of a codeand a collation information output means controls a collation information reception means in accordance with a decoding method of a code contained in pertinent informationand acquires collation information.
[0019]Even when two or more billing addresses of collation information existsuitable collation information corresponding to a code can be acquired.
[0020]
[Embodiment of the Invention]Nextan embodiment of the invention is described with reference to drawings.
[0021]Drawing 1 is a block diagram showing the composition of the information distribution receiving system of a 1st embodiment of this invention.
[0022]The code generation part 101 which is a cipher generation means receives the information for transmissionand an encryption keyand enciphers and outputs the information for transmission. The broadcast transmission section 102 which is a broadcast transmitting means receives the enciphered informationand broadcasts to many and unspecified persons. The center side communications department 103 including an encryption key transmitting means receives an encryption keyand transmits through a channel. The terminal side communications department 104 including an encryption key reception means receives and outputs an encryption key through a channel. The broadcast receive section 105 which is a broadcast receiving means receives and outputs the broadcast information which was enciphered. Although the decoding part 106 which is a decoding means receives the information and encryption key which were enciphered and the information that it decodes is outputtedit does not operatewhen an encryption key is not inputted. Herethe code generation part 101the broadcast transmission section 102and the center side communications department 103 constitute an information distributing deviceand the broadcast receive section 105the terminal side communications department 104and the decoding part 103 constitute the

information reception device.
[0023]Thereforein the system of drawing 1only while communicating and having received the encryption keythe decoding part 106 operates.
[0024]In this systemas long as it corresponds with the code transmitted at that timean encryption key may be changed at arbitrary time. Thereforein a receiverwhile decoding informationit is necessary to always continue receiving an encryption key through a channel.
[0025]Since it is not necessary to send information to the center side from the terminal side as a channelmultiaddress calling besides a general interactive communications service can be used.
[0026]When using the communications service which can check and record that the addressee has received like a telephone network as a channel with the device on communications networkssuch as a switchboardit can check that the addressee has received the encryption key. Thereforewhen charging to informationcharge amount can be determined based on a communication history.
[0027]Drawing 2 is a block diagram showing the composition of the information distribution receiving system of a 2nd embodiment of this invention.
[0028]The information server 201 which is a cipher generation means receives information to transmitenciphersand transmits towards the satellite for broadcast through the sending set 202 which is a broadcast transmitting means. An encryption key is simultaneously sent out to the channel by a dedicated line through the modem 203 which is an encryption key transmitting means. The receiving set 205 which is a broadcast receiving means receives the electric wave from a satelliteand outputs the enciphered information. Simultaneouslythe modem 204 which is an encryption key reception means receives and outputs an encryption key from a channel. The decoding part 206 which is a decoding means decodes the enciphered information using an encryption keyand outputs the information that it decodes. Herethe information server 201the sending set 202and the modem 203 constitute an information distributing deviceand the modem 204the receiving set 205and the decoding part 206 constitute the information reception device.
[0029]The information server 201 changes an encryption key at arbitrary time. Thereforethat a code can be decoded continuously becomes only the information reception device connected to the channel.
[0030]Although the dedicated line was assumed as a channel in the above explanationit is usable also in a usual telephone line and CATV circuit.
[0031]It may be made for the terminal side communications department 105 and the modem 204 to hold an encryption key even after disconnection. In this casedecoding can be continued until an encryption key changes nexteven if it cuts a communication line. When using a telephone line as a communication lineit is useful from a point of telex rate gold reduction.
[0032]Drawing 3 is a block diagram showing the composition of the information distribution receiving system of a 3rd embodiment of this invention.
[0033]The function of the code generation part 301the broadcast transmission

section 302the broadcast receive section 305and the decoding part 308 is the same as the function of the code generation part 101 in drawing 1the broadcast transmission section 102the broadcast receive section 105and the decoding part 106 respectively.

[0034]The collation information generation part 303 receives an encryption keyand generates and outputs the collation information which added arbitrary information to the encryption key. The center side communications department 304 which is a collation information transmitting means receives collation informationand transmits through a channel. The terminal side communications department 306 which is a collation information reception means receives and outputs collation information through a channel. The encryption key extraction part 307 which is encryption key separating mechanism receives collation informationand extracts and outputs an encryption key. The code generation part 301the broadcast transmission section 302the collation information generation part 303and the center side communications department 304 constitute an information distributing device hereand the broadcast receive section 305the terminal side communications department 306the encryption key extraction part 307and the decoding part 308 constitute the information reception device.

[0035]In this systemthe additional information about an encryption key is included in collation informationand it communicates. As additional informationthe time when the encryption key was createdthe shelf-life of an encryption keya decoding algorithm identifierthe service identifier of broadcast servicea purveyor-of-service identifieretc. can be used. When the terminal side communications department 306 can hold collation informationthe shelf-life of the encryption key is included into collation informationand a communication line can be cut until the shelf-life of an encryption key goes out with reference to this by the channel control means of a receiver.

[0036]Drawing 4 is a block diagram showing the composition of the information distribution receiving system of a 4th embodiment of this invention.

[0037]The function of the code generation part 401the broadcast transmission section 402the collation information generation part 403the center side communications department 404the terminal side communications department 406the encryption key extraction part 408the broadcast receive section 405and the decoding part 409respectively The code generation part 301 in drawing 3the broadcast transmission section 302the collation information generation part 303It is the same as that of the function of the center side communications department 304the terminal side communications department 306the encryption key extraction part 307the broadcast receive section 305and the decoding part 308.

[0038]The collating part 407 which is a collation information output means receives pertinent information and collation informationand only when collation information is compared with pertinent information and decoding is permittedit outputs collation information.

[0039]Herethe code generation part 401the broadcast transmission section 402the **** information generating part 403and the center side communications

department 404 constitute an information distributing deviceand the broadcast receive section 405the terminal side communications department 406the collating part 407the encryption key extraction part 408and the decoding part 409 constitute the information reception device.
[0040]Collation information and the pertinent information can use the information in connection with whether decoding of the information enciphered is permitted. For exampleonly when the password sent by collation information and the password entered by pertinent information are in agreementthe usage of permitting decoding is possible. In this casethe password which transmits by collation information transmitsafter performing beforehand the operation in which inverse transformation is impossibleand if it compares with the result of having performed the same operation to pertinent informationthere will be no risk of a password being stolen out of collation informationas generally carried out.
[0041]If connectable [in the system of drawing 3] with a communication line from drawing 1a code can certainly be decodedbut since it can restrict when the addressee has obtained right pertinent information beforehand in the system of drawing 4and it can decodethe addressee of information can be limited more.
[0042]Drawing 5 is a block diagram showing the composition of the information distribution receiving system of a 5th embodiment of this invention.
[0043]The function of the code generation part 501the collation information generation part 503the center side communications department 504the terminal side communications department 505the encryption key extraction part 509and the decoding part 510 each in drawing 4 The code generation part 401the collation information generation part 403the center side communications department 404the terminal side communications department 406the encryption key extraction part 408It is the same as that of the function of the decoding part 409.
[0044]The broadcast transmission section 502 which is a broadcast transmitting means receives the information and pertinent information which were encipheredgenerates a broadcasting signal including bothand broadcasts to many and unspecified persons. The broadcast receive section 506 which is a broadcast receiving means receives and outputs a broadcasting signal. The pertinent information separation part 507 which is pertinent information separating mechanism receives a broadcasting signaland extracts and outputs a code and pertinent information. The collating part 508 which is a collation information output means compares pertinent information with collation informationand only when decoding is permitted by a comparison resultit outputs collation information.
[0045]Herethe code generation part 501the broadcast transmission section 502the collation information generation part 503and the center side communications department 504 constitute an information distributing deviceand the terminal side communications department 505the broadcast communication part 506the pertinent information separation part 507the collating part 508the code extraction part 509and the decoding part 510 constitute the information reception device.
[0046]Pertinent information is information about the information enciphered. For examplethey are an information identifier showing the information included in the

codea numerical value showing the degree of secrecy of informationetc. On the other handcollation information includes decoding permit information [other than an encryption key / pertinent information]. Decoding permit information is information which described the conditions for which an encryption key is used. It is a numerical value etc. which express as an example the degree of secrecy of the information identifier showing one or more informationor the information which can be decoded.

[0047]If the collation information containing the information identifier from which each differs using the collation information generation part 503 two or moreand the degree of information hiding is generated and it transmits using a different communications channelthe information which can decode a receiver can be determined by with which communications channel it connects.

[0048]Drawing 6 is a block diagram showing the composition of the information distribution receiving system of a 6th embodiment of this invention. This system acquires the encryption key of the MPEG 2 packet by which scramble encryption was carried out in CS broadcasting through a channel. Herea telephone line is assumed as a channel. In this systemthe information about the kind of that program is broadcast with a program. On the other handin a channelthe kind of program which can use the encryption key other than an encryption key is transmitted. In a receiverit determines whether decode a code or not according to the kind of this program.

[0049]The timer 601 outputs an encryption key update request for every fixed time. The encryption key generation part 602 will generate and output a new encryption keyif an encryption key update request is received. The collation information generation part 605 adds and outputs the kind of program permitted to an encryption key. Drawing 7 is a figure showing an example of the information about the kind of program used for collation information. The generated collation information is transmitted to a channel through the modem 606. Since it is necessary to transmit collation information to two or more users from one centermultiple address type communications service is used. The code generation part 603 which is a cipher generation means receives an encryption key and MPEG numeralsand generates and outputs a code. The CS broadcasting device 604 which is a broadcast transmitting means receives pertinent information and a codeand broadcasts them through a satellite as a broadcast packet. The information which shows the genre of the program under present broadcast in the same form as drawing 7 is included in pertinent information. The CS receiving set 608 which is a broadcast receiving means receives the broadcast from a satelliteand outputs a broadcast packet. The pertinent information separation part 611 which is pertinent information separating mechanism receives a broadcast packetand separates and outputs pertinent information and a code. The reception side modem 607 receives and outputs collation information from a channel. The collating part 609 which is a collation information output means receives collation information and pertinent informationand if the program genre in pertinent information is contained in the program genre in collation informationit will output

collation information. The encryption key extraction part 610 which is encryption key separating mechanism extracts and outputs an encryption key from collation information. The decoding part 612 which is a decoding means receives a code and an encryption keyand outputs the MPEG numerals produced by decoding a code.
[0050]The timer 601the key generation part 602the code generation part 603the CS broadcasting device 604the collation information generation part 605and the modem 606 constitute an information distributing device hereThe modem 607the CS receiving set 608the collating part 609the encryption key extraction part 610the pertinent information separation part 611and the decoding part 612 constitute the information reception device.
[0051]Although the information about the genre of a program was given to pertinent information and collation information in the above explanationinformation other than a genre can also be given. Drawing 8 is an example which makes possible [decoding] only the program which gave the list of two or more program identifiers to pertinent information at a program identifier and collation informationand was shown in the list. Drawing 9 is an example carried out to the level of a program with which the level of a program is permitted to pertinent information and it permits decoding to collation information by the collation information being givenand only the program below the level being decoded.
[0052]If the telephone number of required multiple address formal ** service is included when collation information comes to hand in pertinent information in drawing 6Collation information is automatically acquirable even if two or more acquisition places of collation information exist according to the purpose by controlling to carry out call origination of the modem 607 to this telephone number.
[0053]
[Effect of the Invention]As explained abovethis invention has the following effects.
(1) Since the invention of claims 1 and 3 can change an encryption key required for decoding of a code frequentlywhen it distributes the enciphered information to many users simultaneouslyits a risk of an inaccurate user decoding or reproducing an encryption key is small.
[0054]Since it can check that the addressee has received the encryption key when it can be checked and recorded with the device on communications networkssuch as a switchboardthat the addressee has received like a telephone network as a channelwhen charging to informationcharge amount can be determined based on a communication history. When this performs paid broadcasting using a scrambler/descramblerit makes it possible to charge only a part to have seen.
(2) The invention of claim 4 can realize the function of the system which consists of claims 1 and 3 by short hour corresponding.
(3) Claim 2 and the invention of 5 and 6 can improve the convenience on employment of a device by communicating additional informationincluding the shelf-life of an encryption keyetc.
(4) When the invention of claims 2 and 7 decodesit can examine by the addressee side whether those who decode are right users.

(5) The invention of claims 89and 10 can be examinedwithout whether a code is a thing corresponding to an encryption keyand decoding. This function can use whether decoding is permitted for a certain specific information to a specific addressee set in order to specify at the transmitting side. For examplethe user who acquires the encryption key through the communications channel of a certain fixed charge amount by paid broadcasting can specify to which program it can view and listen.
(6) The invention of claim 11 can acquire the suitable collation information corresponding to a codeeven when two or more billing addresses of collation information exist.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the information distribution receiving system of a 1st embodiment of this invention.
[Drawing 2]It is a block diagram showing the composition of the information distribution receiving system of a 2nd embodiment of this invention.
[Drawing 3]It is a block diagram showing the composition of the information distribution receiving system of a 3rd embodiment of this invention.
[Drawing 4]It is a block diagram showing the composition of the information distribution receiving system of a 4th embodiment of this invention.
[Drawing 5]It is a block diagram showing the composition of the information distribution receiving system of a 5th embodiment of this invention.
[Drawing 6]It is a block diagram showing the composition of the information distribution receiving system of a 6th embodiment of this invention.
[Drawing 7]It is a figure showing the example of the information included in collation information in a 5th and 6th embodiment of this invention.
[Drawing 8]It is a figure showing an example of operation of the information included in collation information in a 5th and 6th embodiment of this inventionand a collating part.
[Drawing 9]It is a figure showing an example of operation of the information included in collation information in a 5th and 6th embodiment of this inventionand a collating part.
[Description of Notations]
101 Code generation part
102 Broadcast transmission section
103 Center side communications department
104 Terminal side communications department
105 Broadcast receive section
106 Decoding part
201 Information server
202 Sending set

203 Modem
204 Modem
205 Receiving set
206 Decoding device
301 Code generation part
302 Broadcast transmission section
303 Collation information generation part
304 Center side communications department
305 Broadcast receive section
306 Terminal side communications department
307 Encryption key extraction part
308 Decoding part
401 Code generation part
402 Broadcast transmission section
403 Collation information generation part
404 Center side communications department
405 Broadcast receive section
406 Terminal side communications department
407 Collating part
408 Encryption key extraction part
409 Decoding part
501 Code generation part
502 Broadcast transmission section
503 Collation information generation part
504 Center side communications department
505 Terminal side communications department
506 Broadcast receive section
507 Pertinent information separation part
508 Collating part
509 Encryption key extraction part
510 Decoding part
601 Timer
602 Encryption key generation part
603 Code generation part
604 CS broadcasting device
605 Collation information generation part
606 Modem
607 Modem
608 CS receiving set
609 Collating part
610 Encryption key extraction part
611 Pertinent information separation part
612 Decoding part